

**LAW OFFICES OF THOMAS K. CROWE, P.C.**

1250 24th STREET, N.W.  
SUITE 300  
WASHINGTON, D.C. 20037

---

TELEPHONE (202) 263-3640  
FAX (202) 263-3641  
E-MAIL [firm@tkcrowe.com](mailto:firm@tkcrowe.com)

February 29, 2008

**BY ECFS**

Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

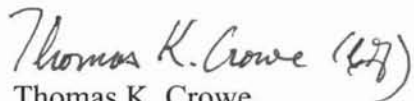
Re: Certification of CPNI Filing; EB Docket No. 06-36

Dear Ms. Dortch:

ECR Voice, LLC, by its undersigned attorney, hereby submits its CPNI compliance certificate and accompanying statement in accordance with Section 64.2009(e) of the Commission's Rules.

Please direct any questions regarding this submission to the undersigned.

Sincerely,

  
Thomas K. Crowe,  
Counsel for ECR Voice, LLC

Enclosures

cc: Federal Communications Commission, Enforcement Bureau, Telecommunications Consumers Division, 445 12th Street, SW, Washington, DC 20554. (via U.S. Mail)

Best Copy and Printing, Inc., [FCC@BCPIWEB.COM](mailto:FCC@BCPIWEB.COM) (via email)

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification  
EB Docket 06-36  
Annual 64.2009(e) CPNI Certification for 2008

**Date filed:** February 27, 2008

**Name of company covered by this certification:** ECR Voice, LLC

**Form 499 Filer ID:** 826283

**Name of signatory:** Marc C. Hawk

**Title of signatory:** President

I, Marc C. Hawk, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



## ***Statement of ECR Voice Customer Proprietary Network Information (“CPNI”) Procedures***

Revised February 2008

ECR Voice (“Company”) is committed to maintaining the privacy and confidentiality of its customers and their personal information. The Company has a CPNI policy set up to comply with the FCC requirements and safeguards to further protect customer information.

Only authorized ECR employees are permitted to have access to customers’ personal information and such access is limited by need. Each and every employee must abide by ECR Voice’s Customer Proprietary Network Information Policy. All ECR employees are required to acknowledge that they understand and will comply with this Customer Proprietary Network Information Policy. Employees who violate the Company’s privacy and security policies are subject to disciplinary action, up to and may include termination.

Vendors and third party contractors have access to confidential customer information only to the extent required for them to perform their services and as outlined within this policy. Outside parties are subject to the same guidelines established by the Company’s policy.

If found that an employee has violated the Company’s CPNI policy, the matter will be taken before the managerial board as to the severity and extent of the issue. Violation may result in suspension of work duties, reassignment to another position, or termination of employment.

Employees and vendors who are discovered to have compromised confidential information will be reported to legal authorities and prosecuted to the fullest extent of the law.

In the event that a breach of CPNI is found, the Company will provide electronic notification of the breach within seven business days to the United States Secret Service (“USSS”) and the Federal Bureau of Investigation (“FBI”) at [www.fcc.gov/eb/CPNI/](http://www.fcc.gov/eb/CPNI/). As requested by the FCC, the Company will then wait another seven business days before notifying the affected customers of the breach unless further requested by the USSS and FBI to postpone the disclosure. However, the Company may notify customers sooner if it is determined that there is a risk of immediate and irreparable harm. Records of discovered breaches will be held by the Company for at least two years.

Each employee of ECR Voice has access to the CPNI policy and has been trained in the requirements of when it is acceptable and not acceptable to use CPNI.

ECR Voice is currently NOT using CPNI to advertise to its customers. The Company will not use such information for its own marketing efforts unless given approval by the customer. If in the event the Company decides to use CPNI for marketing, the Company will first obtain approval from the customer. The Company will follow the requirements and safeguards set by the FCC (*FCC Title 47 CFR 64.2001-9*).

ECR Voice has in place an Executive Committee (consisting of CEO, President, COO & up, Marketing & up, Engineering) that reviews and processes any outbound marketing to ensure compliance with the FCC and the Company CPNI policy.

Regardless of CPNI use, all information received (including CPNI) is held as confidential and will NOT be sold, rented or given to another party unless required by law, requested by the customer, or in providing the service from which the customer information is derived. In the event that a joint venture occurs or an independent contractor is used for marketing communications-related services to the customer, the Company will not disclose a customer’s CPNI without their consent via an “opt- in” response.

Should a customer initiate the release of CPNI via the phone, it will only be released (1) when the customer provides a pre-established password; (2) when the customer requests that the information be sent to the customer's address of record; or (3) when the Company calls the telephone number of record and discloses the information. Should the customer request the release of CPNI at the physical location of the Company, the customer must present a valid photo ID. A valid photo ID would be current identification with picture that is established by the federal government, state, or local authority. (Example: Driver's License, Passport, US Military Card, etc.)

The Company will notify a customer immediately of any account activity, such as a change to a password, an online account or an address of record. Notification may be by voicemail, email or by mail to the customer's address of record.

The Company provides mandatory password protection for online account access. The Company does not base customers' online access solely on a customer's readily available biographical information.

At this point in time, the company does not encrypt its Customers' Proprietary Network Information. It only encrypts customer credit card information. The company is looking into extending the encryption to CPNI.

The Company has set in place to submit an annual certification with the FCC, explaining any actions taken against data brokers and summarizing all consumer complaints received during the year relating to the unauthorized release of CPNI. Along with this certification an officer will sign a compliance certificate each year attesting that the officer has personal knowledge that the Company's procedures are sufficient to ensure compliance with the CPNI rules.